Developing an Undergraduate Information Systems Security Track

Aditya Sharma
asharma@nccu.edu

Marianne C. Murphy
mmurphy@nccu.edu

Mark A. Rosso
mrosso@nccu.edu

Donna Grant
grantd@nccu.edu

Computer Information Systems,
North Carolina Central University
Durham, NC, 27707, USA

ABSTRACT

Information Systems Security as a specialized area of study has mostly been taught at the graduate level. This paper highlights the efforts of establishing an Information Systems (IS) Security track at the undergraduate level. As there were many unanswered questions and concerns regarding the Security curriculum, focus areas, the benefit of certifications, and limited experience of undergraduate students, we reviewed prior literature and conducted in depth semi-structured interviews of industry executives that are responsible for the security portfolio within their organizations. We present findings that can benefit not only our efforts but also other schools that plan to offer similar programs at an undergraduate level.

Keywords: Undergraduate curriculum, Information Systems Security, Information Systems

1. INTRODUCTION

State government budget crises in recent years have led to significant funding cuts to the budgets of many public universities and colleges (Carter, 2012). These budget issues have increased emphasis on accountability measures, including job placement rates (Akey, 2012). For example, the University of North Carolina (UNC) university system requires that "employment opportunities" be considered a basis for establishing new academic programs (UNC, 2008).

In terms of employment opportunities, Information Systems Security, as a program area, would seem to meet this criterion. As computer systems, networks, and network applications proliferate in both corporate and consumer usage, the availability of Security professionals continues to be an issue. For example, a recent study (Ayoub, 2011) forecasts the compound annual growth rate (CAGR) of jobs for Security professionals during the 2010-2015 period to be 13.2% worldwide.

This paper documents the research and decision-making process that one academic department went through to establish an Information Systems Security track in its curriculum. The paper is organized as follows. After more detailed background on our specific circumstances, we summarize the literature on Information Systems Security curriculum development; present our findings from interviews with local Security professionals; and finally, discuss what these findings mean for the Information Systems Security track.

2. BACKGROUND

North Carolina Central University is primarily a liberal arts school with approximately 8,300 students. The School of Business offers a bachelor's of science degree in Computer Information Systems. In 2010, facing serious state funding cuts, the university embarked on a complete and thorough evaluation of all programs. As a result, some programs were cut and others were combined. Schools and faculty were rearranged. By 2011, the School of Business was facing its own challenges with a new dean in an accreditation year. The dean's first initiative is to develop and implement an effective strategic plan for the university. This strategic plan includes evaluating our own programs and realigning with the changing markets and our new strategic initiatives.

Keeping this strategic plan in mind, the Computer Information Systems discipline was assigned its own challenge. Under the direction of the new dean, the Chancellor required the School of Business to develop a new program. As a part of our new program we developed four tracks (Business Analysis, Network Administration, Bioinformatics and IS Security). In establishing the new Information Systems Security track there were still some unanswered questions that were critical to its success. Among the questions we wanted answered initially were:

- Specifically, what content should be in the Security curriculum?
- Should we offer certifications in Security, and if so, which one(s)?
- What should faculty qualifications be to teach courses in the Security track?

3. LITERATURE REVIEW

It has been estimated that today's computer systems are less secure than equivalent systems of just ten years ago, with our systems growing more vulnerable with every passing year (Garfinkel, 2012). Security research scientist Simson Garfinkel (2012) goes on to assert that the issue is not being adequately addressed, as currently "most computer professionals receive little if any training in Security, most CS professors and software engineers try to ignore it, and there are few Security specialists." Swart (2007) agrees that the "lack of inclusion of IT security in the curriculum has led to significant risk for companies."

Program Content in Current Programs

Although the need for higher education institutions to train future computer professionals regarding Security is clear, what is not so clear is the specific content of the curriculum. Even the name of the curricula, and the specific discipline area offering such curricula, vary widely. Names for the field include Information Assurance, Information Security and Computer Security (Wikipedia, 2012), ordered from broad to narrow. Other names include Information Security and Assurance, Network Security (Swart, 2007), Information Systems Security (e.g., Ralevich & Martinovic, 2010) and Cybersecurity (Smith, Koohang, & Behling, 2010). Discipline areas hosting these programs include Business, Computer Science, Computer Engineering (Swart, 2007), Information Science (Ralevich & Martinovic, 2010) Computer Information Systems, and Management Information Systems (Smith, Koohang, & Behling, 2010).

Even within similar program names or discipline areas, there is no standard content for Security in the curriculum (Perez, et al., 2011; Swart, 2007; Whitman & Mattord, 2004, 2006). Programs can specialize in Security, offer a specific course or courses in Security, or integrate Security throughout the curriculum. Courses/programs can focus on technical aspects, managerial aspects or a balance of both (Whitman & Mattord, 2004).

Some programs offer Security certifications by professional bodies, while some don't. With the exception of the CISSP certification (Certified Information Systems Security Professional, offered by the International Information Systems Security Certification Consortium, Inc., (ISC)²®), most certifications focus on the mastery of hands-on, technical skills (Swart, 2007). These certifications tend to be vendor-specific, and are more popular in Associates degree and certification programs (Perez et al., 2011; Swart, 2007; Whitted & Mattord, 2004). However, they often have articulation problems with four-year programs (Perez, et al., 2011). Petrova (et al., 2004) determined that their

bachelor's degree program did not have room for providing a certification opportunity. Finally, it is not clear whether all or any programs need to have some form of certification as the outcome of the program (Cooper et al., 2009).

There are currently no ACM/AIS model curricula for a specialized program in Security. The IS 2010 curriculum model (ACM-AIS, 2010) provides for Security content integrated throughout the curricula, with electives in risk management, and audit and controls. The IT 2008 curriculum model (ACM-IEEE, 2008), which provides for the greatest coverage of Security topics, does not specify the degree of dedicated Security courses versus integration across the curriculum.

Skills Wanted by Industry in Graduates

There is very little research on what IS Security skills employers want colleges and universities to provide in their graduates. Whitted & Mattord (2006) say they get mixed responses from industry advisors to their program, also stating that most businesses have not developed explicit requirements for what it means to be an IS Security professional. After a focus group with local companies, Petrova (et al., 2004) concluded that "employers would prefer to hire IT graduates with broad knowledge but with specialized skills rather than specialists alone." This conclusion was confirmed by Swart (2007), who has performed the most comprehensive research to-date on the Security needs of industry:

> The results from the interview show that the information systems security function has evolved into a business oriented function. Significant time and attention are directed to protecting and educating users of information systems. IS security professionals are responsible for managing risk, demonstrating alignment between the IS security function and overall business objectives, and ensuring compliance with myriad regulations. Traditional IS security responsibilities involving monitoring networks and information systems to detect and respond to intrusions and attacks have not changed. These general results were consistent across each of the subjects interviewed. (pp. 111-112)

Regarding certifications desired by industry, Swart found that industry professionals have a strong preference for the Security Management and Audit focused certifications. This is consistent with the role of the IS Security professional expressed above. However, given that this is one study, done years ago in a rapidly changing field, more research would be useful for the development of academic IS Security programs.

Qualifications for Faculty Teaching Security Courses

One area about which the research literature has much to say, and with general agreement, is that Security curricula increase the difficulty of finding qualified faculty (Cooper, et al., 2009; Ralevich & Martinovic, 2010; Whitted & Mattord, 2004; 2006):

> One of the major constraints to the growth in student numbers is a difficulty in attracting and hiring new faculty with the adequate background and experience in IS security. Most of the experts and practitioners in the field, except for those with the related IS security certification, do not meet the criteria for teaching in the degree program, such as having at least a master's degree in a related field. Universities have a similar problem in recruiting faculty and that is one of the main reasons for a lack of such programs at the undergraduate level in North America or anywhere else. (Ralevich & Matinovic, 2010, p. 311)

Several researchers reported that certifications and conference attendance can be helpful to get four-year institution faculty up-to-speed for teaching Security courses (Frank & Werner, 2011; Ralevich & Martinovic, 2010; Whitted & Mattord, 2004). Due to the increased emphasis on certifications, instructors in associate degree programs are generally certified (Perez, et al, 2011).

4. DATA COLLECTION

Data Collection

In our effort to further understand the current needs in IS Security education we conducted 4 in-depth semi-structured interviews of industry executives who manage security within their organizations.

While a broader range of participants and more interviews would be better, we believe that ours is a representative sample which is sufficient to capture the key dynamics and highlight current trends and needs in IS security. To protect the identity of our respondents we have coded the responses using letters A through D. The

profiles of the interviewees are summarized in Table 1 of the Appendix.

As is consistent with most exploratory qualitative studies most of the questions on the interview were open ended. The data was analyzed by coding the responses and identifying underlying themes and trends that emerged from the interview data. This approach is consistent with the contextual data analysis suggest by Krippendorff (1980).

5. DATA ANALYSIS AND RESULTS

Key themes and findings from the interviews have been summarized in Table 1 and Table 2 of the Appendix.

Based on our interview data we found that all interviewees felt that there is a growing need for security professionals and undergraduate students with limited experience have a good chance of securing employment provided they can demonstrate knowledge of key concepts in the security area.

Among the interviewees two favored a broad approach towards building a security track. According to interviewee C "the program curriculum should be a mile wide and an inch deep, because that will allow students to have their foot in the door. Most employers at the entry level do not expect depth." Interviewee D also favored a broad knowledge of the key areas but also suggested specialization for students in an area of interest. The broad curriculum for security could include common body of knowledge courses covering multiple domains similar to the content covered for CISSP certifications. The target job positions would be entry level positions such as junior network administrator or associate security analyst, threat analyst.

Interviewees A and B favored a more focused approach for the Security track. Their view was that deeper specialization of students allows them to differentiate themselves from the competition. Among the courses suggested for a focused approach were courses on compliance, network security and accounting. The target position for jobs would be Network Specialist, Compliance Specialist or Security Analyst.

All of the interviewees strongly favored certifications for students as an additional strength in the job market. All of them recommended the CISSP as a beneficial certification for students to have. Interviewees A and B also recommended the CCNA certification for students specializing in the networking area.

All of the interviewees strongly encouraged students to be a part of organizations such as the Information Systems Security Association (ISSA). Membership to organizations such as ISSA enables employers to connect with potential recruits and provide great networking opportunities for students.

One of key themes that emerged from all the interviews was that students should be able to understand the role of security within the context of business. According to Interviewee D "Students should have a broad understanding of what security is and what it does for the organization". Besides technical knowledge students should also be able to explain why they need to secure and why in a certain way. As interviewee A put it succinctly "they should be able to explain the why before the how".

Last but not the least all of the interviewees were of the view that having faculty that is certified sends a positive signal to the potential employers about the quality of the program.

6. CONCLUSION

The new program at NCCU has four suggested tracks of study, one of which is the Information Systems Security track.

Two challenges exist in developing an undergraduate degree track in Information Systems security. The first is that the field is quite broad. Every aspect of computer and Management Information Systems involves Information Systems Security. Second, a Security professional must know their "area" well in order to successfully secure it. In other words, in order to be successful, a Security graduate should have a "companion skill" as well (Swart, 2007). Most Security professionals have multiple years of experience in the domain that they eventually work to secure. As interviewee A had mentioned "you need to understand the network topology before you can secure it". All of the interviewees echoed similar concerns. Having domain knowledge assists the security professional to not only "keep the bad guys out" but also to "make sure that the good guys are able to work and get their work done" (Swart, 2007).

Unlike some of the other well-known programs in Security at other schools that are at the graduate level, we at NCCU are striving to build a successful undergraduate program in Security. Our objective is to produce a technically prepared Business professional who could be

employed in the Security area of an organization with minimal experience. The purpose of this research was to interview Security professionals and ascertain key factors that would maximize our student's ability to secure employment and also determine the effectiveness of certifications for students and for faculty on this ability.

For the future we will continue to engage with industry executives and academic partners to build and grow our program into a successful template for undergraduate Security education.

7. REFERENCE

ACM-AIS (2010). IS 2010 Curriculum Guidelines for Undergraduate Degree Programs in Information Systems. Retrieved July 8, 2012 from http://www.acm.org/education/curricula/IS%202010%20ACM%20final.pdf

ACM-IEEE (2008). IT 2008 Curriculum Guidelines for Undergraduate Degree Programs in Information Technology. Retrieved July 8, 2012 from http://www.acm.org//education/curricula/IT2008%20Curriculum.pdf

Akey, L. (2012). Institutional accountability and competition for resources in undergraduate education among U.S. public four-year institutions. Unpublished doctoral dissertation. University of Minnesota.

Ayoub, R. (2011). The 2011 (ISC)2 Global Information Security Workforce Study, Frost & Sullivan. Retrieved July 7, 2012 from https://www.isc2.org/uploadedFiles/Landing_Pages/NO_form/2011GISWS.pdf

Carter, J. (2012). Quality cutting: perceived faculty and staff effects of state budget cuts on institutional quality. Public Organization Review, 12(1), 41-56.

Cooper, S., Nickell, C., Piotrowski, V., Oldfield, B., Abdallah, A., Bishop, M., Caelli, B., Dark, M., Hawthorne, E., Hoffman, L., Pérez, L., Pfleeger, C., Raines, R., Schou, C., and Brynielsson, J. (2009). An exploration of the current state of information assurance education. ACM SIGCSE Bulletin, 41(4), 109–125

Frank, C. and Werner, L. (2011). The value of the CISSP certification for educators and professionals. Proceedings of the 8th Annual Conference on Information Security Curriculum Development, pp. 50-53.

Garfinkel, S. (2012). The cybersecurity risk. Communications of the ACM, 5(8), 29-32.

Krippendorff, K. (1980). Content Analysis: An Introduction to Its Methodology, Sage Publication, Newbury Park, CA.

Pérez, L., Cooper, S., Hawthorne, E. Wetzel, S., Brynielsson, J., Gökce, A., Impagliazzo, J., Khmelevsky, Y., Klee, K., Leary, M., Philips, A., Pohlmann, N., Taylor, B., and Upadhyaya, S. (2011) Information assurance education in two and four-year institutions. ACM ITiCSE-WGR '11: Proceedings of the 16th annual conference reports on Innovation and technology in computer science education, pp. 39-53.

Petrova, K., Philpott, A., Kaskenpalo, P., & Buchan, J. (2004). Embedding information security curricula in existing programmes. Proceedings of the 1st Annual Conference on Information Security Curriculum Development, pp. 20-29.

Ralevich, V. & Martinovic, D. (2010). Designing and implementing an undergraduate program in information systems security. Education and Information Technologies, 15(4), 293-315.

Smith, T., Koohang, A. and Behling, R. (2010). Formulating an effective cybersecurity curriculum. Issues in Information Systems, 11(1), 410-416.

Swart, R. (2007). A framework for the integration of information security and assurance within information systems curricula. Unpublished doctoral dissertation. Utah State University. Retrieved July 8, 2012 from http://gradworks.umi.com/33/06/3306442.html.

UNC. (2008). Policy on Academic Program Planning. The UNC Policy Manual, 400.1. Retrieved July 7, 2012 from http://www.northcarolina.edu/aa_planning/degrees/Board_of_Governors_Policy_on_Academic_Program_Planning.pdf

Whitman, M., & Mattord, H. (2004). Designing and teaching information security curriculum. Proceedings of the 1st Annual

Conference on Information Security Curriculum Development, 1-7.

Whitman, M., & Mattord, H. (2006). Developing the BS-ISA: lessons learned and future directions. Proceedings of the 3rd Annual Conference on Information Security Curriculum Development, 49-51.

Wikipedia. (2012). Information Assurance. Retrieved on July 8, 2012 from http://en.wikipedia.org/wiki/Information_assurance

Appendix

Table 1: Interviewee Outlook on Security Program Recommendations

Inter-viewee	Interviewee Title	Scope	Membership Benefits for students (ISSA etc.)	Courses for Broad Program	Certifica-tions for Instructors	CISSP Benefit in Hiring
A	VP, Security Company	Focused	Yes	NA	Yes	Yes
B	Director, IT Solutions Company	Focused	Yes	NA	Yes	Yes
C	Network Engineer/Security Instructor in Banking and Education	Broad	Yes	Common body of knowledge for CISSP	Yes	Yes
D	Manager - Networking and Security, Telecommunications Company	Both Broad and Focused	Yes	Broad under-standing of security, CISSP Domain	Yes	Yes

Table 2: Interviewee Outlook on Target Positions in Security

Interviewee	Target Positions for Undergraduates	Courses for Target Positions	Certifications Preferred for Target Positions	Job Market for Target Positions
A	Network security, Compliance	Compliance, Basic Accounting, Networking	CCNA, CISSP	Good
B	Network Security specialist	Networking	CCNA, CISSP	Good
C	Threat Analysts, Penetration Testers, Security Analysts	Security courses based on CISSP Domain Knowledge	CISSP	Good
D	Junior Network administrator, Assoc. Security Analyst	Programming, CISSP Domains	CISSP	Good